IN THE CLAIMS

1. (Original) A security framework for supporting kernel-based hypervisors within a computer system, the security framework comprising:

a security master;

one or more security modules; and

a security manager;

wherein the security master and security modules execute in kernel space.

2. (Original) The security framework of claim 1, wherein the security manager executes in user space.

3. (Original) The security framework of claim 1, wherein one of the security modules is designed to apply a security policy to a specific application.

4. (Original) The security framework of claim 1, wherein one of the security modules is designed to apply a security policy to two or more different applications.

5. (Original) The security framework of claim 1, wherein one of the security modules enforces application-specific policy decisions for applications running in user space.

6. (Original) The security framework of claim 5, wherein the security module grants access to one or more computing resources as a function of the application requesting access.

7. (Original) The security framework of claim 5, wherein one of the security modules enforces resource-specific policy decisions for applications running in user space.

8. (Original) The security framework of claim 7, wherein the security module grants access to one or more computing resources as a function of the computing resource being requested.

9. (Original) The security framework of claim 7, wherein one of the security modules is designed to apply a security policy to a specific application.

10. (Original) The security framework of claim 7, wherein one of the security modules is designed to apply a security policy to two or more different applications.

11. (Original) The security framework of claim 1, wherein one of the security modules enforces resource-specific policy decisions for applications running in user space.

12. (Original) The security framework of claim 11, wherein the security module grants access to one or more computing resources as a function of the computing resource being requested.

13. (Original) The security framework of claim 11, wherein one of the security modules is designed to apply a security policy to a specific application.

14. (Original) The security framework of claim 11, wherein one of the security modules is designed to apply a security policy to two or more different applications.

15. (Original) The security framework of claim 11, wherein the security modules are hierarchically configured.

16. (Original) The security framework of claim 1, wherein the security modules are hierarchically configured.

17. (Original) The security framework of claim 1, wherein the security modules are designed so they can be loaded while the computing system is running.

18. (Original) The security framework of claim 1, wherein the security master includes a kernel-based facility for installing, configuring, monitoring and removing security modules.

19. (Original) The security framework of claim 1, wherein the security master includes:

a kernel-based facility for installing, configuring, monitoring and removing security modules; and

entry points for registering a security module, intercepting system calls, releasing system calls, and communicating messages between security modules and user space.

20. (Original) The security framework of claim 1, wherein the security manager includes an interface for communicating with security master, wherein the interface permits a user to configure and control security modules from user space.

21. (Original) The security framework of claim 1, wherein the security manager includes an interface for communicating with security master, wherein the interface permits a user to configure and control security modules from user space, wherein management functions available to the user include:

the ability to list a set of rules that are being enforced by each security module;

the ability to load a new set of rules for a particular security module; and

the ability to log and view activity within the security framework.

22. (Original) The security framework of claim 1, wherein a user daemon executes in user space and allows the security master to initiate actions in user space.

23. (Original) The security framework of claim7, wherein the security master includes a kernel-based facility for installing, configuring, monitoring and removing security modules.

24. (Original) The security framework of claim 7, wherein the security master includes:

a kernel-based facility for installing, configuring, monitoring and removing security modules; and

entry points for registering a security module, intercepting system calls, releasing system calls, and communicating messages between security modules and user space.

25. (Original) The security framework of claim 7, wherein the security manager includes an interface for communicating with security master, wherein the interface permits a user to configure and control security modules from user space.

26. (Original) The security framework of claim 7, wherein the security manager includes an interface for communicating with security master, wherein the interface permits a user to configure and control security modules from user space, wherein management functions available to the user include:

the ability to list a set of rules that are being enforced by each security module;
the ability to load a new set of rules for a particular security module; and
the ability to log and view activity within the security framework.

27. (Original) The security framework of claim 7, wherein a user daemon executes in user space and allows the security master to initiate actions in user space.